(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－215030
（P2002－215030A）
(43)公開日　平成14年７月31日(2002.7.31)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ　５Ｊ１０４
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ

審査請求　有　　請求項の数10　ＯＬ　（全９頁）

(21)出願番号　特願2001－8638(P2001－8638)

(22)出願日　平成13年１月17日(2001.1.17)

(71)出願人　597174182
株式会社高度移動通信セキュリティ技術研究所
神奈川県横浜市港北区新横浜三丁目20番地８

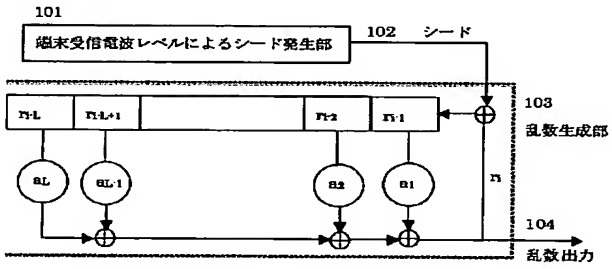
(72)発明者　加藤　武比古
神奈川県横浜市港北区新横浜三丁目20番８号　株式会社高度移動通信セキュリティ技術研究所内

(74)代理人　100099254
弁理士　役　昌明　（外１名）

最終頁に続く

(54)【発明の名称】　乱数発生方法

(57)【要約】
【課題】　移動体端末において、外部操作なしに、簡単な構成で安全な乱数を発生する。
【解決手段】　端末受信電波レベルのように、移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとする。サンプルデータをシード102として乱数生成部103に入力して、乱数104を発生する。ある時点の内部状態がコピーされても、次のタイミングからは同じ乱数を発生しないので安全である。特別の部品・材料の追加も必要とせず、質の良い乱数を発生させることができる。



1

【特許請求の範囲】

【請求項１】　移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとし、前記サンプルデータをシードとして擬似乱数発生手段に入力して、擬似乱数を発生することを特徴とする乱数発生方法。

【請求項２】　前記移動体端末が受信する電波の強度レベルを検出し、前記電波強度レベルを示すデータを前記シードとして用いることを特徴とする請求項１記載の乱数発生方法。

【請求項３】　前記移動体端末の位置を検出し、前記位置を示すデータを前記シードとして用いることを特徴とする請求項１記載の乱数発生方法。

【請求項４】　前記移動体端末の通信内容の一部を所定の方法で抽出してサンプルデータを求め、前記サンプルデータを前記シードとして用いることを特徴とする請求項１記載の乱数発生方法。

【請求項５】　前記移動体端末の電池電圧を検出し、前記電池電圧を示すデータを前記シードとして用いることを特徴とする請求項１記載の乱数発生方法。

【請求項６】　前記移動体端末が受信する電波の強度レベルと、前記移動体端末の位置と、前記移動体端末の通信内容と、前記移動体端末の電池電圧とのうちのいずれか２つ以上の情報を抽出して合成サンプルデータとし、前記合成サンプルデータを前記シードとして用いることを特徴とする請求項１記載の乱数発生方法。

【請求項７】　前記移動体端末が受信する電波の強度レベルと、前記移動体端末の位置と、前記移動体端末の通信内容と、前記移動体端末の電池電圧とのうちのいずれか１つ以上の情報を一定時間ごとにサンプリングしてサンプルデータとし、前記サンプルデータのデジタル値をメモリに蓄積し、前記メモリに蓄積された多倍長のサンプルデータを前記シードとして用いることを特徴とする請求項１記載の乱数発生方法。

【請求項８】　生成したシードをサンプルデータの１つとしてフィードバックして入力し、入力したサンプルデータとフィードバックしたシードとを合成して合成サンプルデータとすることを特徴とする請求項１～７のいずれかに記載の乱数発生方法。

【請求項９】　生成したシードを所定のハッシュ関数により変換してハッシュ化シードとし、前記ハッシュ化シードを前記擬似乱数発生手段に入力することを特徴とする請求項１～８のいずれかに記載の乱数発生方法。

【請求項１０】　前記ハッシュ化シードをサンプルデータの１つとしてフィードバックして入力し、入力したサンプルデータとフィードバックしたシードとを合成して合成サンプルデータとすることを特徴とする請求項９記載の乱数発生方法。

【発明の詳細な説明】

2

【０００１】

【発明の属する技術分野】本発明は、乱数発生方法に関し、特に、暗号方式のパラメータである乱数を効率的に発生する乱数発生方法に関する。

【０００２】

【従来の技術】乱数は、暗号方式上重要なパラメータである。複数の端末がシステムを構成する場合、端末ごとに異なる乱数を発生させる必要がある場合が多い。乱数には、乱数生成器にシードを入力し、乱数生成器内のレジスタによる演算を経て乱数として出力されるものと、ホワイトノイズなどを用いるものがある。

【０００３】従来の乱数発生方法には、

（１）予め機器に設定された初期値をシードとする方法（次のシードには出力された乱数を使用）

（２）乱数が必要な都度シードを取ってきて入力する方法（例えばキーボード入力のような操作の必要な情報をシードとする）

（３）ホワイトノイズなど、物質の特性をシードとして利用する方法

などがある。

【０００４】疑似乱数は、適当な長さの種（シード）から、アルゴリズムに基づいて生成される。図10に示すように、シード発生部1001におけるシード発生源1002からの情報が、Ａ／Ｄ変換部1003においてデジタル化され、これがシード1004として乱数生成部1005に入力される。そして、このシードは、乱数生成部1005でアルゴリズムに基づいて演算され、所定の長さの乱数1006として出力される。

【０００５】図11に、乱数生成部に用いられる線形フィードバックシフトレジスタ（LFSR）を示す。図中の四角い箱1101が、１ビットの情報を記憶できるシフトレジスタのセルであり、単位時間ごとに矢印の向きにシフトする。結線部1102における○の中に書かれているa_iは、結線状態を示しており、$a_i=1$のときは、結ばれていることを示し、$a_i=0$のときは、切断されていることを示す。そして、加算部1103においてビット加算される。LFSR出力特性は、配線a_iにより定まる。LFSRよりさらに複雑性をもたすために、非線形フィードバックシフトレジスタ、フィルタ生成器、組み合わせ生成器などが用いられることもある。

【０００６】従来の乱数発生器では、例えば電源をONしたときに、何らかの初期値をシードとして乱数生成部に設定し、その後はシードの入力がなく、出力した乱数を次のシードとして入力することにより、暗号で必要となる比較的長いビット数の乱数系列を生成する。乱数生成部は、図11に示すような構成である。これらレジスタに初期のシードを設定し、フィードバックにより、このレジスタの内容を書き換えながら乱数を発生させる。この場合、ある時点でのレジスタの設定値と、フィードバックレジスタの構成が分かれば、シードが変わるまでの間

は、発生する乱数が攻撃者に分かってしまう。

【０００７】次に、ホワイトノイズによる乱数発生について説明する。図12に、ホワイトノイズのような物理現象を用いて乱数を発生する方法を示す。ホワイトノイズ1201を、Ａ／Ｄ変換部1202でデジタル化して、乱数生成器を通すことなく、そのまま乱数1203として出力する方法である。この場合、上述のような攻撃の心配はないが、ホワイトノイズを取り出すための特別の部品・材料が必要になる。

【０００８】

【発明が解決しようとする課題】しかしながら、従来のシードを用いる方法では、ある時点でのレジスタの設定値とレジスタの構成が分かれば以降の乱数が攻撃者に分かってしまうという問題がある。また、ホワイトノイズを用いる場合は、特別の部品・材料が必要であるという問題がある。

【０００９】上記（１）で述べた設定値をシードとする方法では、機器の特性あるいは機器に保有されている情報に基づくシードを使うので、全数探索攻撃が可能である。また、ある時点での乱数生成器の設定値と構成が分かれば、以降の乱数は攻撃者に分かってしまう。上記（２）で述べたシードを外部から入力する方法では、（１）に比べて攻撃は難しくはなるものの、定期的な操作が必要であるため、端末のユーザ負担が大きい。安全性のためには、攻撃者に観測または予測できない程度の頻度と内容の操作が必要である。上記（３）で述べたホワイトノイズなどを利用する方法では、ホワイトノイズなどを発生する特別の部品・材料が必要である。このように、従来の暗号発生方法には多くの問題がある。

【００１０】本発明は、上記従来の問題を解決して、ある時点の内部状態がコピーされても、次のタイミングからは同じ乱数を発生することがなく、端末のユーザが意識的に端末を操作する必要もなく、特別の部品・材料の追加なく、すべて携帯端末が保有している機構を用いて乱数を発生できる、簡単で安全な乱数発生方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記の課題を解決するため、本発明では、移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとし、サンプルデータをシードとして擬似乱数発生手段に入力して、擬似乱数を発生する構成とした。このように構成したことにより、簡単な方法で安全な乱数を発生することができる。

【００１２】すなわち、本発明では、移動体端末の性質を活かして、移動体端末にある機能のみを使い、かつ時間的に変化するものをシードとして利用して乱数を発生するので、ある時点の内部状態がコピーされても、次のタイミングからは同じ乱数を発生せず、推測不可能になり、ホワイトノイズ発生器のような特別の部品・材料も必要なくなり、移動する端末の特性により同じ乱数が異なる端末で発生する可能性もなくすことができ、質の良い乱数を発生させることができる。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態について、図１～図９を参照しながら詳細に説明する。

【００１４】（第１の実施の形態）本発明の第１の実施の形態は、移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとし、サンプルデータをシードとして擬似乱数発生手段に入力して、擬似乱数を発生する乱数発生方法である。

【００１５】図１は、本発明の第１の実施の形態における移動体端末の受信レベルをシードとする乱数発生方法を示す図である。図１において、シード発生部101は、移動体端末が受信する電波の強度レベルを検出して抽出したサンプルデータを出力する手段である。シード102は、乱数生成の初期値データである。乱数生成部103は、線形フィードバックシフトレジスタ（LFSR）などにより擬似乱数を生成する手段である。乱数出力104は、乱数生成部の出力データである。

【００１６】図２は、携帯端末の位置情報をシードとする乱数発生方法を示す図である。図２において、シード発生部201は、移動体端末の位置を検出して抽出したサンプルデータを出力する手段である。シード202は、乱数生成の初期値データである。乱数生成部203は、線形フィードバックシフトレジスタ（LFSR）などにより擬似乱数を生成する手段である。乱数出力204は、乱数生成部の出力データである。

【００１７】図３は、携帯端末の通信内容をシードとする乱数発生方法を示す図である。図３において、シード発生部301は、移動体端末の通信内容を検出して抽出したサンプルデータを出力する手段である。シード302は、乱数生成の初期値データである。乱数生成部303は、線形フィードバックシフトレジスタ（LFSR）などにより擬似乱数を生成する手段である。乱数出力304は、乱数生成部の出力データである。

【００１８】図４は、携帯端末の電池電圧をシードとする乱数発生方法を示す図である。図４において、シード発生部401は、移動体端末の電池電圧を検出して抽出したサンプルデータを出力する手段である。シード402は、乱数生成の初期値データである。乱数生成部403は、線形フィードバックシフトレジスタ（LFSR）などにより擬似乱数を生成する手段である。乱数出力404は、乱数生成部の出力データである。

【００１９】図５は、携帯端末の複数の情報をシードとする乱数発生方法を示す図である。図５において、シード発生部501は、複数のサンプルデータを合成して、合成サンプルデータを出力する手段である。端末受信電波

レベル抽出手段502は、移動体端末が受信する電波の強度レベルを検出して抽出したサンプルデータを出力する手段である。端末位置情報抽出手段503は、移動体端末の位置を検出して抽出したサンプルデータを出力する手段である。端末通信内容抽出手段504は、移動体端末の通信内容を検出して抽出したサンプルデータを出力する手段である。電池電圧抽出手段505は、移動体端末の電池電圧を検出して抽出したサンプルデータを出力する手段である。シード506は、乱数生成の初期値データである。乱数生成部507は、線形フィードバックシフトレジスタ（LFSR）などにより擬似乱数を生成する手段である。乱数出力508は、乱数生成部の出力データである。

【００２０】上記のように構成された本発明の第１の実施の形態における乱数発生方法の動作手順を説明する。最初に、図１を参照して、移動体端末の受信レベルをシードとする方法を説明する。移動体端末の受信電波レベルは、絶えず変化しており、再現性はない。図１に示すように、端末受信電波レベルによるシード発生部101で、受信電波のレベルデータを抽出して、サンプルデータを、シード102として出力する。このシード102を、乱数生成部103内のLFSRに入力し、演算を行なって乱数104を生成させる。このシード102と同じ変化を示すものは、他に存在することはない。サンプリングごとにシード102が変化するので、シード102のビット数が少なくても、再現性のない良質の乱数を得ることができる。

【００２１】第２に、図２を参照して、携帯端末の位置情報をシードとする方法を説明する。携帯端末では、移動に伴い位置は絶えず変化しており、位置情報の変化に再現性はない。図２に示すように、位置情報によるシード発生部201で、移動体端末の位置を検出して抽出したサンプルデータを、シード202として出力する。このシード202を、乱数生成部203に入力し、演算を行なって乱数204を生成させる。このシード202と同じ変化を示すものは他に存在することはない。サンプリングごとにシード202が変化するので、シード202のビット数が少なくても、再現性のない良質の乱数を得ることができる。

【００２２】第３に、図３を参照して、携帯端末の通信内容をシードとする方法を説明する。携帯端末では、通話などにより通信内容が絶えず変化しており、通信内容の変化に再現性はない。図３に示すように、通信内容によるシード発生部301で、移動体端末の通信内容を検出して抽出したサンプルデータを、シード302として出力する。このシード302を、乱数生成部303に入力し、演算を行なって乱数304を生成させる。このシード302と同じ変化を示すものは他に存在することはない。サンプリングごとにシード302が変化するので、シード302のビット数が少なくても、再現性のない良質の乱数を得ることができる。

【００２３】第４に、図４を参照して、携帯端末の電池電圧をシードとする方法を説明する。携帯端末では、端

末使用により電池電圧が絶えず変化しており、電池電圧の変化に再現性はない。図４に示すように、電池電圧によるシード発生部401で、移動体端末の電池電圧を検出して抽出したサンプルデータを、シード402として出力する。このシード402を、乱数生成部403に入力し、演算を行なって乱数404を生成させる。このシード402と同じ変化を示すものは他に存在することはない。サンプリングごとにシード402が変化するので、シード402のビット数が少なくても、再現性のない良質の乱数を得ることができる。

【００２４】第５に、図５を参照して、携帯端末の複数の状態情報をシードとする方法を説明する。携帯端末の受信電波強度レベル、端末位置、通信内容、電池電圧は、単独でも再現性なく変化しているが、これらの複数の情報を加算してシードとすることで、変化の状況は一層複雑になり、より再現性がなくなることを利用する。シード発生部501内において、端末受信電波レベル抽出手段502で、移動体端末が受信する電波の強度レベルを検出してサンプルデータを抽出し、端末位置情報抽出手段503で、移動体端末の位置を検出してサンプルデータを抽出し、端末通信内容抽出手段504で、移動体端末の通信内容を検出してサンプルデータを抽出し、電池電圧抽出手段505で、移動体端末の電池電圧を検出してサンプルデータを抽出し、これらの複数のサンプルデータを加算する。これをシード506として乱数生成部507に入力し、演算を行なって乱数508を生成させる。このシード506と同じ変化を示すものは他に存在することはない。サンプリングごとにシード506が変化するので、シード506のビット数が少なくても、再現性のない良質の乱数を得ることができる。

【００２５】上記のように、本発明の第１の実施の形態では、乱数発生方法を、移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとし、サンプルデータをシードとして擬似乱数発生手段に入力して、擬似乱数を発生する構成としたので、簡単な方法で安全な乱数を発生することができる。

【００２６】（第２の実施の形態）本発明の第２の実施の形態は、移動体端末で発生する情報を一定時間ごとにサンプリングしてサンプルデータとし、サンプルデータのデジタル値をメモリに蓄積し、メモリに蓄積された多倍長のサンプルデータをシードとして用いる乱数発生方法である。

【００２７】図６は、本発明の第２の実施の形態における乱数発生方法を示す図である。図６において、シード発生部601は、状態情報を一定時間ごとにサンプリングしたサンプルデータのデジタル値をメモリに蓄積した多倍長のサンプルデータを出力する手段である。端末受信電波レベル抽出手段602は、移動体端末が受信する電波の強度レベルを検出する手段である。タイミング回路60

3は、電波の強度レベル情報を一定時間ごとにサンプリングして抽出する手段である。メモリ604は、サンプルデータのデジタル値を蓄積する手段である。シード605は、乱数生成の初期値データである。乱数生成部606は、線形フィードバックシフトレジスタ（LFSR）などにより擬似乱数を生成する手段である。乱数出力607は、乱数生成部の出力データである。

【００２８】上記のように構成された本発明の第２の実施の形態における乱数発生方法の動作手順を説明する。図６に示すように、シード発生部601において、端末受信電波レベル抽出手段602で、移動体端末が受信する電波の強度レベルを検出し、タイミング回路603で一定時間ごとサンプリングし、これをメモリ604に入力して蓄積する。端末受信電波レベル抽出手段602の代わりに、端末位置、通信内容、電池電圧のデータを抽出する手段を使うこともできる。メモリ604に蓄積されたデータをシード605として乱数生成部606に入力し、演算を行なって乱数607を得る。このシード605と同じ変化を示すものは他に存在することはない。サンプリングごとに変化するデータを複数個連結して、多倍長の長いシード605を得ることができるので、１つのサンプリングデータのビット数が少なくても、再現性のない良質の乱数を得ることができる。

【００２９】上記のように、本発明の第２の実施の形態では、乱数発生方法を、移動体端末で発生する情報を一定時間ごとにサンプリングしてサンプルデータとし、サンプルデータのデジタル値をメモリに蓄積し、メモリに蓄積された多倍長のサンプルデータをシードとして用いる構成としたので、簡単な方法で安全な乱数を発生することができる。

【００３０】（第３の実施の形態）本発明の第３の実施の形態は、シードをフィードバックし、シードを常に変化させる乱数発生方法である。

【００３１】図７は、本発明の第３の実施の形態における乱数発生方法を示す図である。図７において、シード発生部701は、移動体端末の状態を検出して抽出したサンプルデータと、出力したシードの一部を再入力したものを合成して出力する手段である。シード702は、乱数生成の初期値データである。乱数生成部703は、線形フィードバックシフトレジスタ（LFSR）などにより擬似乱数を生成する手段である。乱数出力704は、乱数生成部の出力データである。

【００３２】上記のように構成された本発明の第３の実施の形態における乱数発生方法の動作手順を、図７を参照して説明する。シード発生部701において発生したシード702の一部を、シード発生部701にフィードバックさせる。シード発生部701は、第１の実施の形態で説明した複数のサンプルデータを合成するものと同じである。フィードバック回路は、シード702を、他のサンプルデータと同様にしてシード発生部701に入力する手段である。シード発生部701で合成した結果を、シード702として乱数生成部703に入力し、演算の後、乱数704を得る。端末受信電波レベル、電池電圧などのような、変化の度合いが小さく、ビット長が短い情報であっても、繰り返しフィードバックさせることにより、変化が大きくビット長の長いシードとすることができる。その結果、再現性が一層少ない良質の乱数を生成することができる。

【００３３】上記のように、本発明の第３の実施の形態では、乱数発生方法を、シードをフィードバックし、シードを常に変化させる構成としたので、簡単な方法で安全な乱数を発生することができる。

【００３４】（第４の実施の形態）本発明の第４の実施の形態は、シードにハッシュをかける乱数発生方法である。

【００３５】図８は、本発明の第４の実施の形態における乱数発生方法を示す図である。図８において、シード発生部801は、移動体端末の状態を検出して抽出したサンプルデータを出力する手段である。ハッシュ関数手段802は、入力データを混合して分散する手段である。シード803は、乱数生成の初期値データである。

【００３６】図９は、本発明の第４の実施の形態における乱数発生方法の別の例を示す図である。図９において、シード発生部901は、移動体端末の状態を検出して抽出したサンプルデータと、ハッシュしたシードの一部を再入力したものを合成して出力する手段である。ハッシュ関数手段902は、入力データを混合して分散する手段である。シード903は、乱数生成の初期値データである。

【００３７】上記のように構成された本発明の第４の実施の形態における乱数発生方法の動作手順を説明する。最初に、図８を参照して、ハッシュ関数を利用したシード発生方法を説明する。シード発生部801で発生したシードデータを、ハッシュ関数手段802に入力する。シード発生部801は、第１～第３の実施の形態で説明したものと同じである。ハッシュ関数手段802で、所定のハッシュ関数により、入力データを攪拌して、シード803を発生させる。ハッシュ関数は、入力が１ビットでも異なれば、出力ビットの大半が異なるという性質を持つため、受信レベルや電池電圧のような、変化の度合いが小さくビット長が短い情報であっても、変化が大きくビット長の長いシードとすることができる。その結果、再現性が一層少ない良質の乱数を生成することができる。

【００３８】第２に、図９を参照して、ハッシュをかけたシードを、シード発生部901にフィードバックさせて、より複雑なシードを発生する方法を説明する。シード発生部901において発生したシードデータを、ハッシュ関数手段902に入力する。ハッシュ関数手段902で、所定のハッシュ関数により、入力データを攪拌して、シード903を発生させる。シード903の一部を、シード発生部901にフィードバックさせる。シード発生部901は、第１

の実施の形態で説明した複数のサンプルデータを合成するものと同じである。フィードバック回路は、シード903を、他のサンプルデータと同様にしてシード発生部901に入力する手段である。ハッシュ関数で撹拌してフィードバックしたシードを、変化する状態情報と組み合わせることにより、変化が大きくビット長の長いシードとすることができる。その結果、再現性が一層少ない良質の乱数を生成することができる。

【００３９】上記のように、本発明の第４の実施の形態では、乱数発生方法を、シードにハッシュをかける構成としたので、簡単な方法で安全な乱数を発生することができる。

【００４０】

【発明の効果】以上の説明から明らかなように、本発明では、移動体端末の有する機能手段が発生する状態情報のうちで時間的に不規則に変化する再現性のない情報の一部を抽出してサンプルデータとし、サンプルデータをシードとして擬似乱数発生手段に入力して、擬似乱数を発生する構成としたので、簡単な方法で安全な乱数を発生することができるという効果が得られる。

【００４１】すなわち、携帯端末特有の変化を示す情報よりシードを作成するので、他からその変化を推測することができず、安全である。ある時点でのレジスタの設定値とフィードバックレジスタの構成が攻撃者に分かったとしても、以降の変化する情報をシードとして用いるため、発生する乱数が攻撃者に分かることはない。シードは絶えず変化しているため、ある時点でのシードのビット数が数ビットであっても、規則性のない良質の乱数を得ることができる。

【００４２】携帯端末が保有する機構のみを用いるものであり、特別の部品・材料を必要とすることはなく、端末の使用者が意識して端末を操作する必要がないので、簡単な構成で、操作性のよい乱数発生方法が実現できる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態における端末受信電波レベルをシードとする乱数発生方法を示す図、

【図２】本発明の第１の実施の形態における端末位置情報をシードとする乱数発生方法を示す図、

【図３】本発明の第１の実施の形態における端末通信内容をシードとする乱数発生方法を示す図、

【図４】本発明の第１の実施の形態における電池情報をシードとする乱数発生方法を示す図、

【図５】本発明の第１の実施の形態における複数の情報を加算しシードとする乱数発生方法を示す図、

【図６】本発明の第２の実施の形態におけるシード発生源情報をサンプリングしメモリ蓄積したものをシードとする乱数発生方法を示す図、

【図７】本発明の第３の実施の形態におけるフィードバック回路を有するシード発生部による乱数発生方法を示す図、

【図８】本発明の第４の実施の形態におけるハッシュ関数によるシード発生方法を示す図、

【図９】本発明の第４の実施の形態におけるハッシュ関数と変化するシードを組み合わせたシード発生方法を示す図、

【図１０】従来の乱数発生方法を示す図、

【図１１】従来の線形フィードバックシフトレジスタ（LFSR）を示す図、

【図１２】従来のホワイトノイズによる乱数発生方法を示す図である。

【符号の説明】

101 端末受信電波レベルによるシード発生部
102 シード
103 乱数生成部
104 乱数出力
201 端末位置情報によるシード発生部
202 シード
203 乱数生成部
204 乱数出力
301 端末通信内容によるシード発生部
302 シード
303 乱数生成部
304 乱数出力
401 電池電圧によるシード発生部
402 シード
403 乱数生成部
404 乱数出力
501 シード発生部
502 端末受信電波レベル抽出手段
503 端末位置情報抽出手段
504 端末通信内容抽出手段
505 電池電圧抽出手段
506 シード
507 乱数生成部
508 乱数出力
601 シード発生部
602 端末受信電波レベル抽出手段
603 タイミング回路
604 メモリ
605 シード
606 乱数生成部
607 乱数出力
701 シード発生部
702 シード
703 乱数生成部
704 乱数出力
801 シード発生部
802 ハッシュ関数
803 シード

11

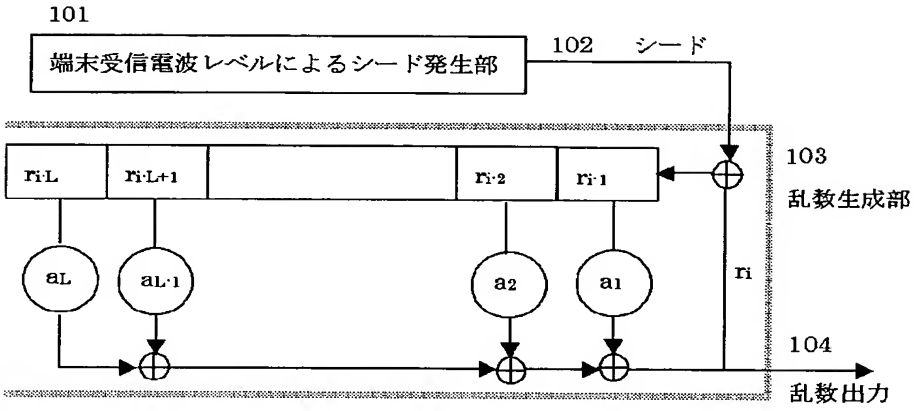
901　シード発生部
902　ハッシュ関数
903　シード
1001　シード発生部
1002　シード発生源
1003　Ａ／Ｄ変換部
1004　シード
1005　乱数生成部

12

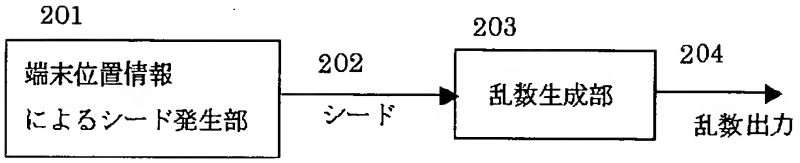
*1006　乱数出力
1101　シフトレジスタ
1102　結線部
1103　加算部
1201　ホワイトノイズ発生部
1202　Ａ／Ｄ変換部
1203　乱数出力

*

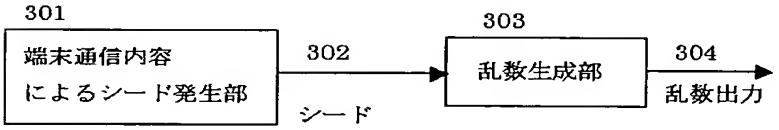
【図１】



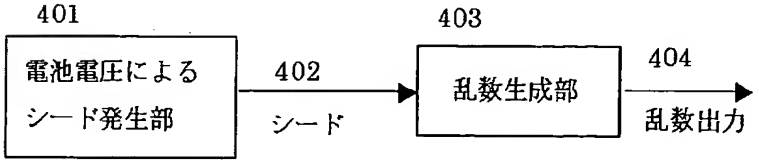
【図２】



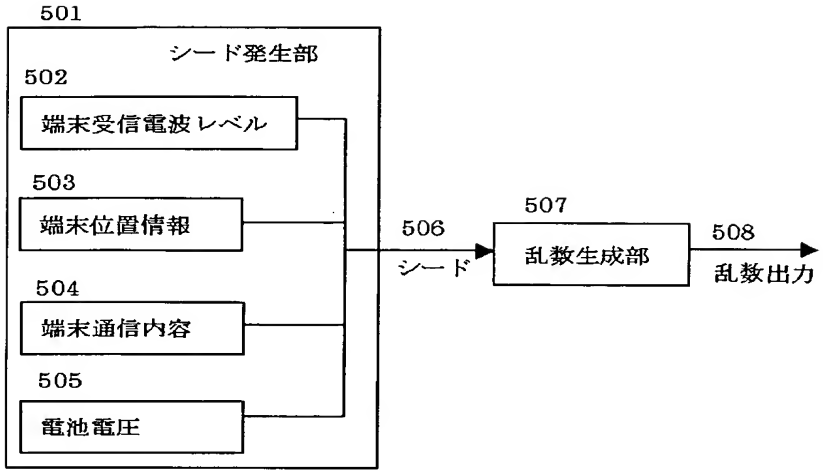
【図３】



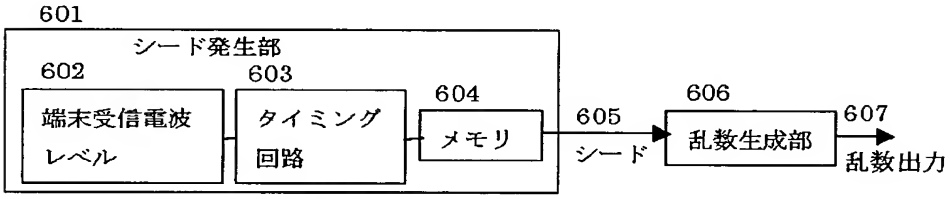
【図４】



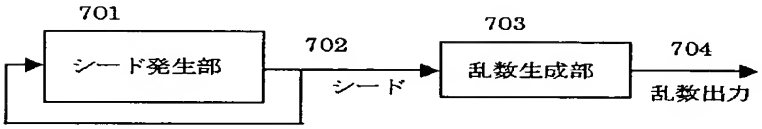
【図５】



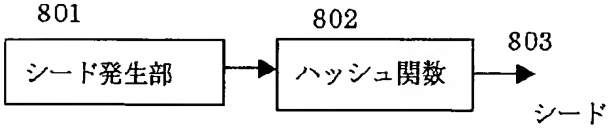
【図６】



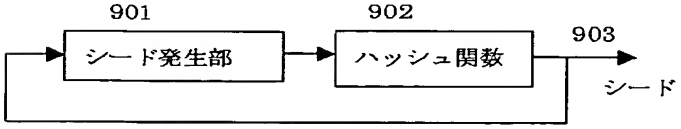
【図７】



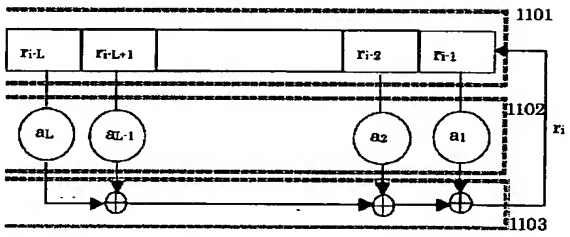
【図８】



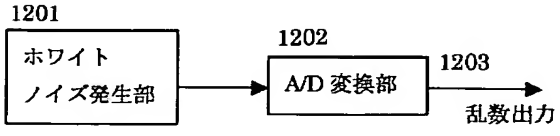
【図９】



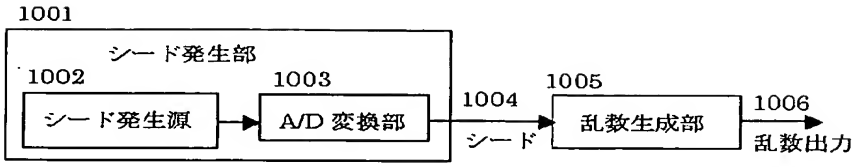
【図１１】



【図１２】



【図１０】



フロントページの続き

(72) 発明者　松崎　なつめ
神奈川県横浜市港北区新横浜三丁目20番８号　株式会社高度移動通信セキュリティ技術研究所内

(72) 発明者　安齋　潤
神奈川県横浜市港北区新横浜三丁目20番８号　株式会社高度移動通信セキュリティ技術研究所内

(72) 発明者　松本　勉
神奈川県横浜市青葉区柿の木台13－45

Ｆターム(参考)　5J104 AA41 FA01 GA01 GA04 NA04 NA12 NA23